Homeland Security

INCIDENT HANDLING OVERVIEW FOR ELECTION OFFICIALS

Incident Handling Overview for Election Officials

This document provides election officials with cyber incident handling steps to assist with incident readiness and the incident response services that the Department of Homeland Security National Protection and Programs Directorate can provide, by request, through its National Cybersecurity and Communications Integration Center.

NOTE: If you are experiencing or suspect malicious cyber behavior, contact the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCICCustomerService@hq.dhs.gov

NCCIC INCIDENT RESPONSE TEAM SERVICES

Once you request assistance from the NCCIC Incident Response Team (IRT), we will work with you and provide the following capabilities and services, as needed.

- **Incident triage**: In order to best understand the severity of the incident, first we scope the incident and determine what resources are required.
- **Network topology review**: This is an assessment of network structure with recommendations, including potential access points (ingress and egress), remote access, segmentation, and interconnectivity.
- **Infrastructure configuration review**: Analysis of core devices on the network that are or can be used for network security. Log analysis is used to determine possible malicious activity.
- **Incident specific risk overview**: Provide tailored products and in-person briefings for technical, program manager, or senior leadership audiences on the specifics of the incident in question.
- **Hunt analysis**: We deploy tools which identify evidence of compromise, potential for persistent adversarial access, and detect indicators of compromise.
- **Security Program Review**: A review of the client's existing security roles, responsibilities, and policies.
- **Digital media analysis**: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators to prevent future attacks.
- **Malware analysis**: Reverse engineering of malware artifacts to determine functionality and build indicators to prevent future attacks.

To request these services, please contact NCCICCustomerService@hq.dhs.gov.

Homeland Security

Incident Handling Overview for Election Officials

INCIDENT RESPONSE PLANNING

No one can predict when or how severe an incident will be, however, there are a few best practices we suggest so that you are better positioned to handle a cybersecurity incident.

- Develop a comprehensive Incident Response Plan that includes:
  - Command Center, if needed, as single point of channeled communications
    - Dedicated resources, as needed, including supplies and equipment
  - Adaptability to different types of incidents, severity
  - Assigned roles and responsibilities of the response team, as well as backups so that each person knows exactly what is expected should an incident occur
  - Communication decision tree
  - Procedures to include:
- Log book which will detail the information that is needed to be collected per incident
- Notification schedule, including point(s) of contact with the most up-to-date contact information.
- Contact information should include: Up, Lateral, Down – per State, County, or Local
- Exercise incident response procedures
  - Conduct table top exercises
  - Simulate forensic scenarios, practice collecting forensic data
  - Make sure your team is trained and comfortable with all tools to ensure they are well versed to use in high pressure scenarios.
  - Have a sample press release written so that you can distribute to your stakeholders should an incident occur.

Homeland Security

Incident Handling Overview for Election Officials

CHECKLIST FOR REQUESTING ASSISTANCE FROM OUR CYBER INCIDENT RESPONSE TEAM

Do you suspect an incident has occurred? Review the checklist below, these are common questions we will ask upon your request.

- Are you reporting an active incident or has it already occurred? ☐ **Active** ☐ **Previous**
- Has Law Enforcement been contacted? ☐ **Yes** ☐ **No**
  - If yes, who? PoC, contact information
- Do you have a third party vendor working with you on this incident? ☐ **Yes** ☐ **No**
  - If yes, who? PoC, contact information
- Do you know the initial vector of attack? ☐ **Yes** ☐ **No**
  - If yes, where?
- Do you know where on your network potentially malicious activity was observed? ☐ **Yes** ☐ **No**
  - If yes, where?
- Do you believe infrastructure to cast or tally votes has been affected? ☐ **Yes** ☐ **No**
- Do you have any indicators of compromise from this incident? ☐ **Yes** ☐ **No**
  - If yes, are you able to provide the IRT with copies? (examples: domains, IP addresses, files, suspected malware)
- Do you have current and historical log data? ☐ **Yes** ☐ **No**
  - If yes, you should preserve the log data for further analysis. This includes any network and host based logs.
- Has any of the hosts that are potentially compromised been powered down? ☐ **Yes** ☐ **No**
  - If no, please leave the hosts online and powered on until we can discuss further with you.
- Do you have the ability to take a live forensic memory capture and disc image of compromised or potentially compromised host(s)? ☐ **Yes** ☐ **No**
- Do you have a recovery point objective (usually identified in an Incident Response Plan or Continuity of Operations Plan)? ☐ **Yes** ☐ **No**
  - If yes, do you know how long is it going to take you recover?
- What is the total number of endpoints on your network?

Homeland Security

Incident Handling Overview for Election Officials

INCIDENT RESPONSE OVERVIEW

After requesting assistance from our team, we will likely undertake a process that includes or recommends actions for the following practices:

- **Incident Identification**
  - Fully scope the incident before making any mitigation efforts
  - Capture live forensic data and collect logs
  - Analyze data to understand lateral movement and persistence mechanisms
  - Determine business impact
  - Determine whether the adversary is still present
- **Incident Containment**
  - Closely monitor compromised systems
  - Isolate compromised network systems
  - Limit scope and magnitude of intrusion
  - Gain visibility into the adversary's foothold
    - Setup alerts for known malicious network infrastructure
    - Setup alerts for known compromised accounts
    - Setup alerts for known host-level Tactics, Techniques and Procedures
  - Create containment and eradication strategy
- **Incident Eradication**
  - Remove compromised machines
  - Alert/Block known malicious infrastructure
  - Reset user account passwords
  - De-privilege user accounts
  - Reset service account passwords (difficult!)
  - Implement additional controls
  - Execute all steps concurrently
- **Incident Recovery**
  - Rebuild compromised hosts offline
  - Validate and restore data
  - Continue to monitor compromised systems and accounts

Once recovered from an incident, many organizations benefit from implementing the following practices:

- Conduct an after action assessment (lessons learned)
- Identify what worked during the incident response process and identify breakdowns or gaps
- Create a comprehensive post-incident report
- Revise policies, procedures, incident response plans, etc.
- Create new signatures to detect this type of malicious activity
- Identify areas to improve security posture
- Submit incident and recommendations report to leadership

Homeland Security

Incident Handling Overview for Election Officials

COMMON MISTAKES IN INCIDENT HANDLING

Over the years we have seen mistakes that could have easily been avoided – check out our list and the impact those mistakes can have while handling an incident.

- Mitigating the affected systems before responders can protect and recover data
  - Can cause the loss of volatile data such as memory and other host based artifacts.
  - Adversary will notice and change Tactics, Techniques and Procedures.
- Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)
  - These actions can tip off the adversary that they have been detected.
- Preemptively blocking adversary infrastructure
  - Network infrastructure is fairly inexpensive. Adversary can easily change to new command and control infrastructure and you will lose visibility of their activity.
- Preemptive Password Resets
  - Adversary likely has multiple credentials, or worse, and has access to your entire active directory.
  - Adversary will use other credentials, create new credentials, or forge tickets.
- Failure to preserve or collect log data that could be critical to identifying access to the compromised systems
  - Learn what log types would be critical to an investigation in your organization.
    - Collect and retain these logs for as long as possible.

Homeland Security

Incident Handling Overview for Election Officials

NOTES:

Homeland Security

INCIDENT HANDLING OVERVIEW FOR ELECTION OFFICIALS

Homeland Security